STATE OF ALABAMA

Information Technology Standard

Standard 660-02S1: Laptop Security

1. INTRODUCTION:

A mobile workforce poses unique security challenges. Key mobile security concerns include connecting to un-trusted wired and wireless networks, exposure of sensitive information, and lost or stolen devices. Mobile systems must be configured to provide host-based security as the primary defensive measure, combined with the capability to securely connect from trusted or un-trusted sources. Proper security and configuration of the laptop will reduce the risk of physical theft, malicious logic, and data loss, and implementation of secure connectivity mechanisms will protect remote access into the trusted network by authorized users and reduce the risk of unauthorized access.

2. OBJECTIVE:

Uniform application of baseline laptop security requirements across the State enterprise.

3. SCOPE:

These requirements apply to administrators, managers, and users of State of Alabama laptop, notebook, tablet PC, and similar computer devices (hereafter referred to collectively as “laptops” or “devices”) used to connect to State networks.

4. REQUIREMENTS:

The following requirements are based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-46: Security for Telecommuting and Broadband Communications, and other best practices.

4.1 SECURE CONFIGURATION

Prior to processing State information on a laptop the Information Security Officer (ISO) shall ensure the device (including associated peripheral devices, operating system, applications, network connection methods, and services) complies with applicable state standards and agency requirements and is accredited by an agency-designated authorizing official.

System and network administrator personnel shall establish written procedures and a testing methodology to ensure that all devices are appropriately configured before granting access to State network resources. Procedures shall be performed on an isolated test environment.

Procedures shall address/ensure the following:

4.1.1 Operating System

Ensure the laptop operating system is secured in accordance with the applicable client operating system security baseline.

4.1.2 Patch/Vulnerability Management

Ensure the latest operating system and third-party application patches are installed.

4.1.3 Firewall

Use a host-based firewall or intrusion prevention software to deter intruders and malicious logic from entering the system via an un-trusted connection (then subsequently entering the State network when the system is returned to the local network).

Never use free or trial-use host-based firewalls as much of the functionality required to adequately protect or manage the granularity of the firewall rules is non-existent.

4.1.4 Virus/Malware Protection

All laptop devices shall utilize virus prevention and detection software and have the virus detection signature files updated in accordance with State virus protection standards.

Use host-based adware/spyware prevention software (where possible).

4.1.5 Other Configuration Controls

Laptops shall comply with all applicable State IT policies and standards including but not limited to wireless security, log management, and those policies and standards addressing the subjects listed above. In addition:

- Secure or disable file and printer sharing
- Utilize full-disk encryption (FDE) to protect all data on State-owned laptop devices
- Use a password protected screensaver to lock the device during periods of inactivity
- Disable peer-to-peer (ad-hoc) networking capabilities, if so equipped, to prevent inadvertent peer-to-peer communications

4.2 SECURE CONNECTIVITY

Laptops shall utilize a Virtual Private Network (VPN) to remotely connect to the State network or direct dial connection to State-provided Remote Access Servers (VPN connectivity is the preferred connection method). VPN use and configuration shall comply with State VPN standards.

Secure Sockets Layer (SSL) access to email (e.g., Outlook Web Access) or data access using application layer security through a “thin client” (e.g., CITRIX) are acceptable alternatives to VPN access (unless access to the state backbone is a requirement).

Remote access connectivity shall comply with applicable state policy and standards.

Ensure wired network interfaces (e.g., Ethernet) are disconnected or otherwise disabled when wireless network connections are being used. Similarly, disable the wireless function when connected to a wired network. This ensures the device cannot be accidentally or intentionally used as a bridging or routing device between two or more networks.

4.3 PHYSICAL SAFEGUARDS

4.3.1 Required

Secure the laptop. Use a cable lock or alarm. Attach the locking cable to an immovable or unbreakable object. If leaving a laptop overnight, lock the entrance(s) to the room. If the room cannot be locked then secure the laptop in a locked cabinet or safe.

Eject access card devices and peripheral storage devices from the laptop and secure them separately.

Never leave a laptop in a vehicle.

4.3.2 Recommended

According to the FBI, 97% of unmarked computers are never recovered. Marking the device may increase the chances of having it returned and may also deter casual thieves. Asset tag or engrave the device by permanently marking (or engraving) the outer case or an accessible internal area with the agency name, address, and phone number.

Include a “Return to Sender” text file on the default drive. This will not deter theft, but it may increase the chances of the device being returned in the event it is found, turned-in for maintenance, or retrieved in the course of an investigation.

Use a non-descript carrying case rather than a laptop case displaying the manufacturer's logo. Consider using a form-fitting padded sleeve for the laptop and carrying it in a backpack, courier bag, briefcase, or other common non-descript carrying case. Close and lock the zippers of the case so no one can simply reach in and remove the laptop.

Use privacy screens in public facilities or open, high-traffic environments to prevent “shoulder-surfing” when on-screen data needs to be kept private.

4.4 LOST DEVICES

User shall immediately report the loss of any laptop to their manager, IT Manager, or ISO. Additionally, since network administrative accounts could be cached on the device while it was connected to the host network, the system administrator must change any local network administrative authenticators that may have been used on the lost device.

Recovered devices shall be treated as compromised. Do not connect a previously lost device to any operational network or system until the device has been properly sanitized. There is a significant risk in transferring any user or operational data from the system since there are numerous methods to install and hide malicious code.

4.5 TRAVEL

Air travel: Keep the laptop in sight at all times, especially through security checkpoints where the laptop may precede you through security scanners.

Public hotspots and wireless LANs (WLAN) installed at airports, hotels, and other establishments present high security risks. Wireless encryption and access controls on the laptop often need to be disabled before connecting to a public WLAN, thus, any information exchanged is sent unencrypted. Furthermore the device may be subject to probes and scanning from other clients connected to the WLAN, therefore, the following protective measures shall be followed:

- Do not use a public WLAN unless it is absolutely necessary
- Use a VPN (otherwise all messages can be intercepted)
- Use a personal firewall and ensure its settings are set for maximum protection
- Upon leaving the WLAN, immediately restore all security settings and scan the device for viruses and other malware

Do not download software or applications while on travel. If software updates are required while on travel, virus-scan all software or downloads before installing onto the device.

The longer a system remains disconnected from its supporting infrastructure, the greater the risks of the system being compromised. Therefore, when the risks of un-patched systems are greater than the threats posed by elevated user privileges, consider granting users privileged-level accesses so they are able to manage and update their own system during extended or remote absences.

Any device that has been on travel or was connected to an external or un-trusted network shall be checked for compliance with security policies prior to gaining access to State network resources.

4.6 AWARENESS & TRAINING

Laptop users shall be provided awareness level training (in accordance with State standards) on the security vulnerabilities presented by use of such devices and on appropriate use.

Users with privileged-level accesses shall receive performance level training to ensure they have the knowledge and skills necessary to update and manage the security of their system.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Standard 610-01S1: Cyber Security Awareness & Training

Information Technology Standard 640-02S1: Remote Access Controls

Information Technology Standard 640-02S2: Virtual Private Networks

Information Technology Standard 640-03S2: Wireless Clients

Information Technology Standard 670-04S1: Virus Protection

Information Technology Standard 680-03S1: Encryption

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	1/30/2008	